Remarks/Arguments

Claims 1 to 13 and 36 to 49 remain pending in the application and are subject to discussion. No claim is amended in the present Response to Office Action.

Claim rejection under 35 U.S.C. § 103(a)

Over Shimizu et al. (US 6,085,323) in view of Al-Salqan (US 6,775,382)

Claims 1 to 13 and 36 to 49 are rejected under 35 U.S.C. § 103(a). The Applicant believes the rejections to be improper in view of the following arguments:

The Office Action (page 2, last paragraph and page 3, first paragraph) states that Shimizu teaches:

> "the SIPS of the sender selecting one of a plurality of second keys corresponding to the information dependent on the identity of the receiver and a unique identifier corresponding to said selected second key, said identifier and said corresponding selected second key being known by the SIPS of the receiver (i.e., key selection, column 14, lines 15-30)".

The Applicant respectfully disagrees. According to the Applicant's understanding of the reading of Shimizu, it is true that it is taught to select one of a plurality of second keys; what is essentially the designation of a master key, but it lacks to link the selection of that second key to a unique identifier corresponding to the selected second key and being known by the SIPS of the receiver. Shimizu, in figure 11 and in column 14, lines 15 to 34, makes a reference to that unique identifier as a "KEY ID" that simply corresponds to a *primary key*, which is well known in database management. The information that is also transmitted is the master key designation information, illustrated as the USER INFORMATION on Figure 11. Thus, Shimizu does not teach nor suggested that this KEY ID, the *primary key* is transmitted, and even less that the information is common between the sender's device and the receiver's device.

Accordingly, the Applicant believes that the interpretation of the unique identifier expressed in the Office Action conducts to an inappropriate rejection of claims 1 to 13 and 36 to 49.

The Office Action further states that Shimizu is silent on "encrypting corresponding key identifier using a public key to generate a secure key identifier" and that it would be obvious to one having ordinary skill in the art to employ the teachings of Al-Salqan with the system of Shimizu in order to enhance the security of the system of the latter, the Applicant respectfully disagrees with the opinion of obviousness to teach.

When evaluating the Al-Salqan's method for recovering encryption session keys, one having ordinary skill in the art would understand to use a continuously built database that is fed with the session keys integrated into messages' headers. That database is managed by the certificate authority system and does not involve sharing any information between secured systems. One of ordinary skill in the art, when trying to improve the security of the security level of Shimizu's system would be lead to the communication of some information to a certificate authority system, not to the definition of common information divided in two distinct secure systems. Furthermore, the goal of the two systems are very different: one is to improve security of the communications between a sender and a receiver without the involvement of a certificate authority system, while the other is a method for **recovering encryption keys** in case one of the communication participants looses or forgets his private key.

In view of the above arguments, it is the Applicant's opinion that it would not be obvious to someone of ordinary skill in the art to enhance the security of Shimizu with something taught by Al-Salqan, but would rather require that the person of ordinary skill in the art perform investigation and development to find out how to implement a method including "encrypting correspondent key identifier using a public key to generate a secure key identifier" and managing these correspondent key identifiers in a practical manner.

The Applicant submits that all other claims rejected or otherwise allowable herein not discussed, recite similar limitations to which similar arguments are applicable and thus should be found allowable.

In view of the foregoing arguments, the claim rejections under 35 U.S.C. § 103(a) are deemed improper. Reconsideration of the claim rejections is respectfully requested and allowance of claims 1 to 13 and 36 to 49 at an early date is solicited.

In the event that there are any questions concerning the Response to Office Action or the application in general, the Examiner is respectfully urged to telephone the undersigned so that prosecution of this application may be expedited.

Respectfully,

Denis Bisson et al.

/C. Marc Benoit/
C. Marc Benoît, Reg. No. 50,200
Tel: (450) 646-9997
Customer Number: 31831